PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-205307
(43)Date of publication of application : 30.07.1999

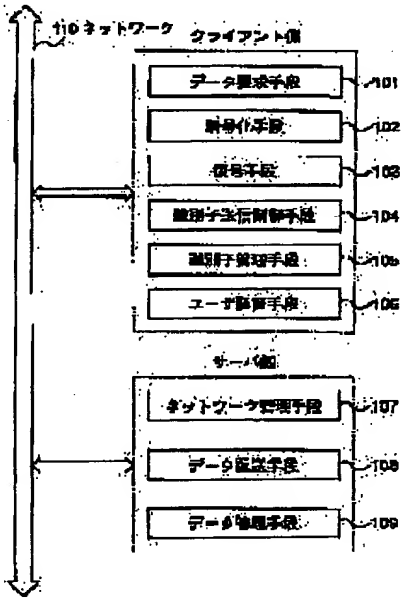
(51)Int.Cl. H04L 9/32
G06F 13/00
// G09C 1/00

(21)Application number : 10-018281
(22)Date of filing : 16.01.1998

(71)Applicant : CANON INC
(72)Inventor : TANAKA TETSUO

(54) INFORMATION PROCESSOR, NETWORK SYSTEM, RESOURCE IDENTIFIER CONVERSION METHOD AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To save the procedure of ciphering and deciphering and to save the distribution procedure of a public key or a secret key by ciphering a resource identifier for specifying data on a network and deciphering it, based on a decipher key.
SOLUTION: An identifier management means 105 is operated so as to urge the input of a ciphered resource identifier (URL) and send the inputted and ciphered URL to a deciphering means 103. The deciphering means 103 deciphers the original URL from the ciphered URL and the decipher key, and if the deciphered URL is correct, delivers it to a client program. In the case the deciphering is not correctly performed or the deciphered URL is not correct, information for indicating incorrect user ID information is sent to the client program. Then, in the case the correct URL is delivered, protocol information, the host information of a server program and resource information on the server program, etc., are fetched so as to obtain a network resource, communication is performed with the server program and the network resource is obtained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－205307

(43)公開日　平成11年(1999)７月30日

(51)Int.Cl.°	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｚ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ
// Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｇ

審査請求　未請求　請求項の数24　ＦＤ　(全 16 頁)

(21)出願番号　特願平10－18281

(22)出願日　平成10年(1998)１月16日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　田中　哲郎
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

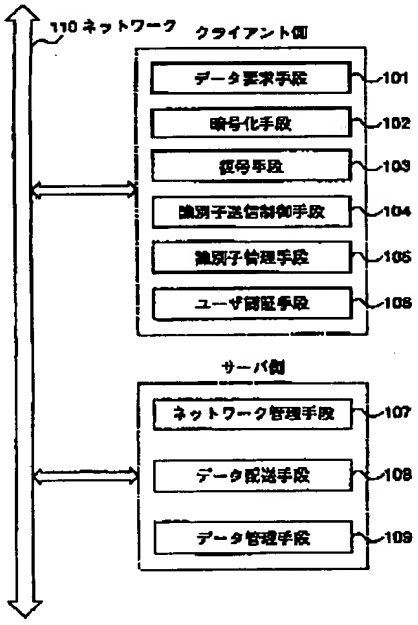
(74)代理人　弁理士　渡部　敏彦

(54)【発明の名称】　情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体

(57)【要約】

【課題】　暗号鍵により暗号化されたリソース識別子を公開し、復号鍵及び元のリソース識別子をユーザ以外には非公開とすることにより、復号鍵により暗号化されたリソース識別子を復号できるユーザにのみアクセス可能にし、暗号化及び復号の手続きや認証のための公開鍵または秘密鍵を配布する手続きを節約すること等を可能とした情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体を提供する。

【解決手段】　サーバにリソース識別子を用いデータ配送を要求するデータ要求手段１０１と、リソース識別子を暗号化する暗号化手段１０２と、リソース識別子を復号する復号手段１０３と、復号したリソース識別子が正しい時はサーバに送信し、正しくない時は送信しない識別子送信制御手段１０４と、入力されたリソース識別子を読取り記憶する識別子管理手段１０５とを有する。



【特許請求の範囲】

【請求項１】 ネットワークを介してサーバと通信可能な情報処理装置であって、
前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とする情報処理装置。

【請求項２】 前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有することを特徴とする請求項１記載の情報処理装置。

【請求項３】 ユーザの認証を行うユーザ認証手段を有することを特徴とする請求項１又は２記載の情報処理装置。

【請求項４】 前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする請求項３記載の情報処理装置。

【請求項５】 パスワードを復号鍵として記憶可能であることを特徴とする請求項１乃至４の何れかに記載の情報処理装置。

【請求項６】 リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段を有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであることを特徴とする請求項１乃至５の何れかに記載の情報処理装置。

【請求項７】 ネットワークを介してサーバ及びクライアント間で通信可能なネットワークシステムであって、
前記クライアント側は、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とするネットワークシステム。

【請求項８】 前記クライアント側は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有し、前記サーバ側は、前記ネットワークの上位装置名、アドレス、通信手段を管理するネットワーク管理手段と、該ネットワーク管理手段による通信でデータを配送するデータ配送手段と、サーバ上のデータを管理するデータ管理手段とを有することを特徴とする請求項７記載のネットワークシステム。

【請求項９】 前記クライアント側は、ユーザの認証を行うユーザ認証手段を有することを特徴とする請求項７又は８記載のネットワークシステム。

【請求項１０】 前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする請求項９記載のネットワークシステム。

【請求項１１】 前記クライアント側は、パスワードを復号鍵として記憶可能であることを特徴とする請求項７乃至１０の何れかに記載のネットワークシステム。

【請求項１２】 前記クライアント側は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段を有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであることを特徴とする請求項７乃至１１の何れかに記載のネットワークシステム。

【請求項１３】 ネットワークを介してサーバと通信可能な情報処理装置におけるリソース識別子変換方法であって、
前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有することを特徴とするリソース識別子変換方法。

【請求項１４】 前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする請求項１３記載のリソース識別子変換方法。

【請求項１５】 ユーザの認証を行うユーザ認証ステップを有することを特徴とする請求項１３又は１４記載のリソース識別子変換方法。

【請求項１６】 前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介し

てリソースを得られない場合はユーザを認証しないことを特徴とする請求項１５記載のリソース識別子変換方法。

【請求項１７】 パスワードを復号鍵として記憶可能であることを特徴とする請求項１３乃至１６の何れかに記載のリソース識別子変換方法。

【請求項１８】 リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理ステップを有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであることを特徴とする請求項１３乃至１７の何れかに記載のリソース識別子変換方法。

【請求項１９】 ネットワークを介してサーバと通信可能な情報処理装置に供給可能な記憶媒体であって、
前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するプログラムを記憶したことを特徴とする記憶媒体。

【請求項２０】 前記プログラムは、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする請求項１９記載の記憶媒体。

【請求項２１】 前記プログラムは、ユーザの認証を行うユーザ認証ステップを有することを特徴とする請求項１９又は２０記載の記憶媒体。

【請求項２２】 前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする請求項２１記載の記憶媒体。

【請求項２３】 パスワードを復号鍵として記憶可能であることを特徴とする請求項１９乃至２２の何れかに記載の記憶媒体。

【請求項２４】 前記プログラムは、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理ステップを有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであることを特徴とする請求項１９乃至２３の何れかに記載の記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体に係り、更に詳しくは、クライアント・サーバ方式によりネットワークを介してデータを送受信する場合に用いて好適な情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体に関する。

【０００２】

【従来の技術】従来、インターネットを介したデータ送受信方法は、ＴＣＰ（TransmissionControl Protocol：ネットワークのトランスポート層の通信プロトコル）／ＵＤＰ（User Datagram Protocol：信頼性を保証しないトランスポート層の通信プロトコル）／ＩＰ（Internet Protocol：インターネット層の通信プロトコル）上のプロトコルを利用したプログラムを使用して行われてきた。その際、ネットワーク上のリソースは、＜プロトコルの種類、リソースを提供するサーバを指定する識別子、サーバ上のリソースを指定する識別子＞からなる組により決定されている。

【０００３】また、サーバのポート番号やサーバ上のユーザ名及び暗号化されたパスワード等の情報も付加的に指定することができる。特に、リソース識別子としてＵＲＬ（Uniform Resource Locator：World Wide Webサーバのアドレス）を利用した場合には、
ｓｃｈｅｍｅ：／／ｕｓｅｒ：ｐａｓｓｗｏｒｄ@ｈｏｓｔ：ｐｏｒｔ／ｕｒｌ－ｐａｔｈ
のように、スキーム（ｓｃｈｅｍｅ）と呼ぶプロトコルの種類を指定する部分と、ユーザ名を指定するユーザ（ｕｓｅｒ）部、パスワードを指定するパスワード（ｐａｓｓｗｏｒｄ）部、ホスト名を指定するホスト（ｈｏｓｔ）部、ポート番号を指定するポート（ｐｏｒｔ）部、サーバ上のリソースを指定するＵＲＬパス（ｕｒｌ－ｐａｔｈ）部、により構成されている。但し、ユーザ部、パスワード部、ポート部、ＵＲＬパス部は、デフォルトとして予め指定されているものを使用する場合はそれぞれ省略可能である。

【０００４】また、インターネットを介したデータ送受信において情報のセキュリティを高めるためには、プロトコル自体に暗号化及び認証機能を付加したり、データそのものを暗号化したりするように構成されている。また、通常のプロトコルを使用してデータそのものを暗号化しない方法として、パスワードを利用した認証機能がある。これは、リソース識別子を指定してリソースを得る際に、ユーザを確認する文字列の入力を促し、正しい文字列が入力された場合にリソースを送信するものである。

【０００５】

【発明が解決しようとする課題】しかしながら、上述した従来技術では、パスワードを付けたリソース識別子（ＵＲＬ）にアクセスする場合、クライアントからサーバにリソース識別子（ＵＲＬ）が送信されると、サーバ

からクライアントにユーザ確認の応答が返され、次に、クライアントはユーザに対して、ユーザ名やパスワード等を入力するためのパネル等を表示してユーザ名やパスワード等を得ていた。正しくユーザ名やパスワード等を得られた場合は、クライアントはサーバにユーザ名やパスワード等を送信し、サーバは送信されたユーザ名やパスワード等を確認し、認証された場合に、認証情報と所望のリソースを送信していた。

【０００６】また、従来技術では、パスワードを付けたリソース識別子（ＵＲＬ）にアクセスする場合、暗号化機能を付加したプロトコルを利用するか、またはデータを暗号化する方法を除いて、パスワードそのものが暗号化されずにネットワークを流れるという欠点があった。そのため、ネットワークを流れるパケットを盗聴することにより悪意のあるユーザによりパスワードが盗まれる恐れがあった。更に、従来技術では、パスワードを付けたリソース識別子（ＵＲＬ）にアクセスする場合、アクセス毎またはセッション毎にパスワードを入力する必要があった。

【０００７】即ち、上述した如く従来技術においては、リソース識別子が暗号化されていないため、認証を行うためには、サーバ側のパスワード機構やクライアント側のサイトのアドレス等を検査して認証を行う必要があった。また、リソース識別子とユーザのディジタル署名機構が独立であったため、ユーザの認証を行うためには、プロトコル自体に暗号化及び認証機能を付加した技術が必要であった。また、データを暗号化して送受信する場合には、復号鍵の配送やデータの復号を行う必要があった。

【０００８】本発明は、上述した点に鑑みなされたものであり、暗号鍵により暗号化されたリソース識別子（ＵＲＬ）を公開し、復号鍵及び元のリソース識別子（ＵＲＬ）をユーザ以外には非公開とすることにより、復号鍵により暗号化されたリソース識別子（ＵＲＬ）を復号できるユーザにのみアクセス可能にし、暗号化及び復号の手続きや認証のための公開鍵または秘密鍵を配布する手続きを簡約すること等を可能とした情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体を提供することを第１の目的とする。

【０００９】また、本発明は、上述した点に鑑みなされたものであり、暗号化されたリソース識別子（ＵＲＬ）を使用する際に、特定のソフトウエアを使用するように強制することにより、ソフトウエアが暗号化鍵及び復号鍵を管理し、ネットワーク上のリソースを送受信すると共に、ユーザのライセンス処理をも同時に行うことを可能とした情報処理装置及びネットワークシステム並びにリソース識別子変換方法及び記憶媒体を提供することを第２の目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するため、請求項１の発明は、ネットワークを介してサーバと通信可能な情報処理装置であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とする。

【００１１】上記目的を達成するため、請求項２の発明は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有することを特徴とする。

【００１２】上記目的を達成するため、請求項３の発明は、ユーザの認証を行うユーザ認証手段を有することを特徴とする。

【００１３】上記目的を達成するため、請求項４の発明は、前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

【００１４】上記目的を達成するため、請求項５の発明は、パスワードを復号鍵として記憶可能であることを特徴とする。

【００１５】上記目的を達成するため、請求項６の発明は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段を有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであることを特徴とする。

【００１６】上記目的を達成するため、請求項７の発明は、ネットワークを介してサーバ及びクライアント間で通信可能なネットワークシステムであって、前記クライアント側は、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有することを特徴とする。

【００１７】上記目的を達成するため、請求項８の発明は、前記クライアント側は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有し、前記サーバ側は、前記ネットワークの上位装置名、アドレス、通信手段を管理するネットワーク管理手段と、該ネットワーク管理手

段による通信でデータを配送するデータ配送手段と、サーバ上のデータを管理するデータ管理手段とを有することを特徴とする。

【００１８】上記目的を達成するため、請求項９の発明は、前記クライアント側は、ユーザの認証を行うユーザ認証手段を有することを特徴とする。

【００１９】上記目的を達成するため、請求項１０の発明は、前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

【００２０】上記目的を達成するため、請求項１１の発明は、前記クライアント側は、パスワードを復号鍵として記憶可能であることを特徴とする。

【００２１】上記目的を達成するため、請求項１２の発明は、前記クライアント側は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段を有し、前記リソース識別子は、Ｗｏｒｌｄ ＷｉｄｅＷｅｂサーバのアドレスを示すＵＲＬであることを特徴とする。

【００２２】上記目的を達成するため、請求項１３の発明は、ネットワークを介してサーバと通信可能な情報処理装置におけるリソース識別子変換方法であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有することを特徴とする。

【００２３】上記目的を達成するため、請求項１４の発明は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする。

【００２４】上記目的を達成するため、請求項１５の発明は、ユーザの認証を行うユーザ認証ステップを有することを特徴とする。

【００２５】上記目的を達成するため、請求項１６の発明は、前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

【００２６】上記目的を達成するため、請求項１７の発明は、パスワードを復号鍵として記憶可能であることを特徴とする。

【００２７】上記目的を達成するため、請求項１８の発明は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理ステップを有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであることを特徴とする。

【００２８】上記目的を達成するため、請求項１９の発明は、ネットワークを介してサーバと通信可能な情報処理装置に供給可能な記憶媒体であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するプログラムを記憶したことを特徴とする。

【００２９】上記目的を達成するため、請求項２０の発明は、前記プログラムは、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有することを特徴とする。

【００３０】上記目的を達成するため、請求項２１の発明は、前記プログラムは、ユーザの認証を行うユーザ認証ステップを有することを特徴とする。

【００３１】上記目的を達成するため、請求項２２の発明は、前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないことを特徴とする。

【００３２】上記目的を達成するため、請求項２３の発明は、パスワードを復号鍵として記憶可能であることを特徴とする。

【００３３】上記目的を達成するため、請求項２４の発明は、前記プログラムは、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理ステップを有し、前記リソース識別子は、Ｗｏｒｌｄ ＷｉｄｅＷｅｂサーバのアドレスを示すＵＲＬであることを特徴とする。

【００３４】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【００３５】［１］第１の実施の形態
図２は本発明の第１の実施の形態及び後述する第２の実施の形態に係る情報処理装置（クライアント）の構成を示すブロック図である。本発明の第１の実施の形態に係る情報処理装置は、入力部２０１と、中央演算処理部２０２と、主記憶部２０３と、読み出し専用メモリ２０４と、二次記憶部２０５と、出力部２０６と、ネットワークインタフェース２０７とを備える構成となっている。
【００３６】上記各部の構成を詳述すると、入力部２０１は、キーボードやマウス等から構成されており、各種データの入力や指示を行う際に使用される。中央演算処理部２０２は、入力部２０１、主記憶部２０３、読み出し専用メモリ２０４、二次記憶部２０５、出力部２０６、ネットワークインタフェース２０７を統括的に制御するものであり、後述する図３のクライアントプログラム３０１、暗号化プログラム３０２、復号プログラム３０４の実行等を制御することにより、後述する図４及び図５のフローチャートに示す処理を実行する。
【００３７】主記憶部２０３は、中央演算処理部２０２による命令実行やデータ操作等を行う際に使用される記憶部である。読み出し専用メモリ２０４は、システムプログラム等を記憶する読み出し専用の記憶部である。二次記憶部２０５は、例えばハードディスク或いはフロッピディスク等から構成されており、主記憶部２０３の容量不足を補う補助記憶部である。出力部２０６は、端末やプリンタ等から構成されており、データの表示や印刷等の出力を行う。ネットワークインタフェース２０７は、ネットワーク上に接続された外部装置との間におけるデータの送受信を行う。
【００３８】図３は本発明の第１の実施の形態及び後述する第２の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムの構成を示すブロック図である。本発明の第１の実施の形態に係るネットワークシステムは、クライアントプログラム３０１、暗号化プログラム３０２、暗号化鍵Ｅ・３０３、復号プログラム３０４、復号鍵Ｄ・３０５、ネットワークインタフェース３０６、ネットワーク３０７、ネットワークインタフェース３０８、サーバプログラム３０９、送信データ３１０から構成されている。クライアント側は、クライアントプログラム３０１～ネットワークインタフェース３０６を備えており、サーバ側は、ネットワークインタフェース３０８、サーバプログラム３０９を備えている。
【００３９】上記各部の構成を詳述すると、クライアントプログラム３０１は、ネットワーク３０７を介してサーバ側から送信されてくるデータを受信する機能を有するプログラムである。暗号化プログラム３０２は、リソース識別子（ＵＲＬ）を暗号化するプログラムである。暗号化鍵Ｅ・３０３は、リソース識別子（ＵＲＬ）の暗号化に使用する。復号プログラム３０４は、暗号化されたリソース識別子（ＵＲＬ）を復号する復号プログラムである。復号鍵Ｄ・３０５は、リソース識別子（ＵＲＬ）の復号に使用する。ネットワークインタフェース３０６は、クライアント側のネットワークインタフェースであり、ネットワーク３０７を介してサーバ側とデータの送受信を行う。
【００４０】ネットワーク３０７は、クライアント及びサーバ間におけるデータの通信経路である。ネットワークインタフェース３０８は、サーバ側のネットワークインタフェースであり、ネットワーク３０７を介してクライアント側とデータの送受信を行う。サーバプログラム３０９は、ネットワーク３０７を介してサーバ側からクライアント側へデータを送信する機能を有するプログラムである。送信データ３１０は、サーバ側からクライアント側へ送信されるデータである。
【００４１】図１は本発明の第１の実施の形態及び後述する第２の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムの要部の構成を示すと共に特許請求の範囲に対応させた機能ブロック図である。情報処理装置（クライアント）は、データ要求手段１０１、暗号化手段１０２、復号手段１０３、識別子送信制御手段１０４、識別子管理手段１０５、ユーザ認証手段１０６を備え、外部装置（サーバ）は、ネットワーク管理手段１０７、データ配送手段１０８、データ管理手段１０９を備えている。この場合、ユーザ認証手段１０６以外の各手段は第１及び第２の実施の形態に共通の構成要件であり、ユーザ認証手段１０６は第２の実施の形態に係る構成要件である。尚、図１の構成は一例であり図示の構成に限定されるものではない。
【００４２】上記各部の機能を詳述すると、クライアント側のデータ要求手段１０１は、サーバに対してＵＲＬ等のネットワーク１１０上のデータを指定するリソース識別子を用いてデータ配送を要求する。暗号化手段１０２は、ネットワーク１１０上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する。復号手段１０３は、暗号化したデータまたはデータを指定するリソース識別子を復号鍵に基づき復号する。識別子送信制御手段１０４は、復号したリソース識別子が正しい場合はリソース識別子をサーバに送信し、復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない。識別子管理手段１０５は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する。
【００４３】また、サーバ側のネットワーク管理手段１０７は、ネットワーク１１０のホスト名、アドレス、通信手段の管理を行う。データ配送手段１０８は、ネットワーク管理手段１０７を用いて通信することによりデータの配送を行う。データ管理手段１０９は、サーバ上のデータの管理を行う。

【００４４】尚、データ要求手段１０１、識別子送信制御手段１０４、識別子管理手段１０５、ユーザ認証手段１０６は、上記図３のクライアントプログラム３０１に対応し、暗号化手段１０２は、上記図３の暗号化プログラム３０２に対応し、復号手段１０３は、上記図３の復号プログラム３０４に対応する。また、ネットワーク管理手段１０７、データ配送手段１０８、データ管理手段１０９は、上記図３のサーバプログラム３０９に対応する。

【００４５】図７は本発明の第１の実施の形態及び後述する第２の実施の形態に係るプログラム及び関連データが記憶媒体から情報処理装置へ供給される概念例を示す説明図である。本発明のプログラム及び関連データは、記憶媒体７０１（例えばフロッピディスク或いはＣＤ－ＲＯＭ等）を情報処理装置７０２に装備された記憶媒体ドライブの挿入口７０３に挿入することで供給される。

【００４６】本発明のプログラム及び関連データを記憶媒体７０１から一旦、二次記憶部２０５（例えばハードディスク）へインストールすることにより、二次記憶部２０５から主記憶部２０３（例えばＲＡＭ）にロードし、本発明のプログラムを実行することが可能となる。但し、二次記憶部２０５へインストールせずに直接、記憶媒体７０１から主記憶部２０３にロードし、本発明のプログラムを実行することも可能である。

【００４７】図６は本発明の第１の実施の形態及び後述する第２の実施の形態に係るプログラム及び関連データを記憶した記憶媒体の記憶内容の構成例を示す説明図である。記憶媒体（フロッピディスク或いはＣＤ－ＲＯＭ等）は、例えばボリューム情報６０１、ディレクトリ情報６０２、プログラム実行ファイル６０３、プログラム関連データファイル６０４等の記憶内容で構成される。本発明のプログラムは、後述する図４及び図５のフローチャートに基づきプログラムコード化されたものである。

【００４８】次に、上記の如く構成してなる本発明の第１の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムにおける情報処理装置（クライアント）の中央演算処理部２０２により制御されるクライアント側の処理の流れについて、図４のフローチャートを参照しながら説明する。

【００４９】情報処理装置（クライアント）側のクライアントプログラム３０１は、本処理が開始すると開始したユーザに対して、暗号化プログラム３０２により暗号化鍵３０３を用いて暗号化されたリソース識別子（ＵＲＬ）を入力するウインドウを表示する（ステップＳ４０１）。次に、暗号化されたリソース識別子（ＵＲＬ）が得られたか否かを判断する（ステップＳ４０２）。暗号化されたリソース識別子（ＵＲＬ）が得られない場合は、本処理を終了する。他方、暗号化されたリソース識別子（ＵＲＬ）が得られた場合は、復号鍵３０５を得る（ステップＳ４０３）。

【００５０】復号プログラム３０４は、暗号化されたリソース識別子（ＵＲＬ）を復号鍵３０５を使用して復号する（ステップＳ４０４）。次に、復号したリソース識別子（ＵＲＬ）からプロトコル情報やサーバ情報やサーバのリソース情報を得て、サーバプログラム３０９とネットワーク３０７を介してサーバ側と通信を行う（ステップＳ４０５）。次に、サーバプログラム３０９との通信により、上記復号したリソース識別子（ＵＲＬ）で指定したデータをサーバ側から得られたか否かを判断する（ステップＳ４０６）。

【００５１】上記復号したリソース識別子（ＵＲＬ）で指定したデータをサーバ側から得られなかった場合は、本処理を終了する。他方、上記復号したリソース識別子（ＵＲＬ）で指定したデータをサーバ側から得られた場合は、リソース識別子（ＵＲＬ）から得られたデータをネットワークのリソースとして表示し（ステップＳ４０７）、本処理を終了する。

【００５２】以上説明したように、本発明の第１の実施の形態によれば、ネットワークシステムの情報処理装置は、サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段１０１と、ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段１０２と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段１０３と、復号したリソース識別子が正しい場合はリソース識別子をサーバに送信し、復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段１０４と、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段１０５とを有するため、下記のような効果を奏する。

【００５３】上記の構成により、本発明の第１の実施の形態では、識別子管理手段１０５は、クライアントプログラムを使用するユーザに対して、暗号化されたリソース識別子（ＵＲＬ）の入力を促し、入力され暗号化されたリソース識別子（ＵＲＬ）を復号手段１０３に送るように動作する。復号手段１０３は、暗号化されたリソース識別子（ＵＲＬ）と復号鍵から元のリソース識別子（ＵＲＬ）を復号し、復号されたリソース識別子（ＵＲＬ）が正しいものである場合には、クライアントプログラムに正しいリソース識別子（ＵＲＬ）を渡すように動作する。

【００５４】上記暗号化されたリソース識別子（ＵＲＬ）から正しく復号されない場合、または復号されたリソース識別子（ＵＲＬ）情報が正しいものでない場合には、不正なユーザＩＤ情報を示す情報をクライアントプログラムに送るように動作する。クライアントプログラムは、正しいリソース識別子（ＵＲＬ）情報を渡された

場合には、リソース識別子（ＵＲＬ）情報から、ネットワークリソースを得るためのプロトコル情報やサーバプログラムのホスト情報、サーバプログラム上のリソース情報等を取り出し、サーバプログラムと通信し、ネットワークリソースを得るように動作する。

【００５５】従って、本発明の第１の実施の形態の効果を箇条書きにすると下記のようになる。

【００５６】（１）データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できるという効果がある。また、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【００５７】（２）パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子（ＵＲＬ）を使用する場合は、クライアントがリソース識別子（ＵＲＬ）を復号し、正しければ復号したリソース識別子（ＵＲＬ）をサーバに送信し、正しくなければリソース識別子（ＵＲＬ）を送信しないため、通信回数が軽減されるという効果がある。

【００５８】（３）パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【００５９】（４）パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子（ＵＲＬ）と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【００６０】（５）パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【００６１】（６）パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【００６２】［２］第２の実施の形態

本発明の第２の実施の形態に係る情報処理装置（クライアント）は、上記第１の実施の形態と同様に、入力部２０１と、中央演算処理部２０２と、主記憶部２０３と、読み出し専用メモリ２０４と、二次記憶部２０５と、出力部２０６と、ネットワークインタフェース２０７とを備える構成となっている（上記図２参照）。

【００６３】また、本発明の第２の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムは、上記第１の実施の形態と同様に、クライアントプログラム３０１、暗号化プログラム３０２、暗号化鍵Ｅ・３０３、復号プログラム３０４、復号鍵Ｄ・３０５、ネットワークインタフェース３０６、ネットワーク３０７、ネットワークインタフェース３０８、サーバプログラム３０９、送信データ３１０から構成されている（上記図３参照）。

【００６４】また、本発明の第２の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）から構成されると共に特許請求の範囲に対応させたネットワークシステムの情報処理装置（クライアント）は、データ要求手段１０１、暗号化手段１０２、復号手段１０３、識別子送信制御手段１０４、識別子管理手段１０５、ユーザ認証手段１０６を備え、外部装置（サーバ）は、ネットワーク管理手段１０７、データ配送手段１０８、データ管理手段１０９を備えている（上記図１参照）。即ち、第２の実施の形態の情報処理装置（クライアント）は、上記第１の実施の形態の各手段１０１～１０５にユーザ認証手段１０６を追加した構成となっている。

【００６５】ユーザ認証手段１０６は、暗号化されたリソース識別子が正しく復号された場合で且つ復号されたリソース識別子からネットワーク１１０を介してリソースを得られた場合はユーザを認証し、暗号化されたリソース識別子が得られない場合、または暗号化されたリソース識別子が正しく復号されない場合、または復号されたリソース識別子からネットワーク１１０を介してリソースを得られない場合はユーザを認証しない。

【００６６】また、本発明の第２の実施の形態に係る処理プログラム及び関連データは、上記第１の実施の形態と同様に、記憶媒体７０１（例えばフロッピディスク或いはＣＤ－ＲＯＭ等）を情報処理装置７０２に装備された記憶媒体ドライブ７０３に挿入することで供給される（上記図７参照）。

【００６７】また、本発明の第２の実施の形態に係る処理プログラム及び関連データを記憶した記憶媒体（フロッピディスク或いはＣＤ－ＲＯＭ等）は、上記第１の実施の形態と同様に、例えばボリューム情報６０１、ディレクトリ情報６０２、プログラム実行ファイル６０３、プログラム関連データファイル６０４等の記憶内容で構成される（上記図６参照）。上記の図１～図３、図６～図７の各部の構成は上記第１の実施の形態で詳述したので説明を省略する。

【００６８】次に、上記の如く構成してなる本発明の第２の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムにおける情報処理装置（クライアント）の中央演算処理部２０２により制御されるクライアント側の処理の流れに

ついて、図５のフローチャートを参照しながら説明する。

【００６９】情報処理装置（クライアント）側のクライアントプログラム３０１は、本処理が開始すると開始したユーザに対して、暗号化プログラム３０２により暗号化鍵３０３を用いて暗号化されたリソース識別子（ＵＲＬ）を入力するウインドウを表示する（ステップＳ５０１）。次に、暗号化されたリソース識別子（ＵＲＬ）が得られたか否かを判断する（ステップＳ５０２）。暗号化されたリソース識別子（ＵＲＬ）が得られない場合は、ステップＳ５０８へ移行する。他方、暗号化されたリソース識別子（ＵＲＬ）が得られた場合は、復号鍵３０５を得る（ステップＳ５０３）。

【００７０】復号プログラム３０４は、暗号化されたリソース識別子（ＵＲＬ）を復号鍵３０５を使用して復号する（ステップＳ５０４）。次に、復号したリソース識別子（ＵＲＬ）からプロトコル情報やサーバ情報やサーバのリソース情報を得て、サーバプログラム３０９とネットワーク３０７を介してサーバ側と通信を行う（ステップＳ５０６）。次に、サーバプログラム３０９との通信により、上記復号したリソース識別子（ＵＲＬ）で指定したデータをサーバ側から得られたか否かを判断する（ステップＳ５０６）。

【００７１】上記復号したリソース識別子（ＵＲＬ）で指定したデータをサーバ側から得られた場合は、ユーザの認証を行う（ステップＳ５０７）。更に、リソース識別子（ＵＲＬ）から得られたデータをネットワークのリソースとして表示し（ステップＳ５０９）、本処理を終了する。他方、上記復号したリソース識別子（ＵＲＬ）で指定したデータをサーバ側から得られなかった場合は、ユーザの認証を行わず（ステップＳ５０８）、本処理を終了する。

【００７２】以上説明したように、本発明の第２の実施の形態によれば、ネットワークシステムの情報処理装置は、サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段１０１と、ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段１０２と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段１０３と、復号したリソース識別子が正しい場合はリソース識別子をサーバに送信し、復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段１０４と、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段１０５と、暗号化したリソース識別子が正しく復号された場合で且つ復号したリソース識別子からネットワークを介してリソースを得られた場合はユーザを認証し、暗号化したリソース識別子が得られない場合、または暗号化したリソース識別子が正しく復号されない場合、または復号したリソース識別子からネットワークを介してリソースを得られない場合はユーザを認証しないユーザ認証手段１０６とを有するため、下記のような効果を奏する。

【００７３】上記の構成により、本発明の第２の実施の形態では、上記第１の実施の形態と同様の動作を行うと共に、更に、上記のユーザ認証手段１０６は、上記の如く、暗号化されたリソース識別子（ＵＲＬ）が正しく復号された場合、且つ復号されたリソース識別子（ＵＲＬ）からネットワークを介してリソースを得られた場合にユーザを認証し、暗号化されたリソース識別子（ＵＲＬ）が得られない場合、または暗号化されたリソース識別子（ＵＲＬ）が正しく復号されない場合、または復号されたリソース識別子（ＵＲＬ）からネットワークを介してリソースを得られない場合にユーザを認証しないように動作する。

【００７４】従って、本発明の第２の実施の形態の効果を箇条書きにすると上記第１の実施の形態と同様に下記のようになる。

【００７５】（１）データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できるという効果がある。また、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【００７６】（２）パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子（ＵＲＬ）を使用する場合は、クライアントがリソース識別子（ＵＲＬ）を復号し、正しければ復号したリソース識別子（ＵＲＬ）をサーバに送信し、正しくなければリソース識別子（ＵＲＬ）を送信しないため、通信回数が軽減されるという効果がある。

【００７７】（３）パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【００７８】（４）パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子（ＵＲＬ）と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【００７９】（５）パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるとい

う効果がある。

【００８０】（６）パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【００８１】尚、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。前述した実施形態の機能を実現するソフトウエアのプログラムコードを記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【００８２】この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００８３】プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【００８４】また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００８５】更に、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００８６】

【発明の効果】以上説明したように、請求項１の発明によれば、ネットワークを介してサーバと通信可能な情報処理装置であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有するため、下記のような効果を奏する。

【００８７】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【００８８】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【００８９】請求項２の発明によれば、情報処理装置は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有するため、下記のような効果を奏する。

【００９０】上記請求項１の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【００９１】請求項３の発明によれば、情報処理装置は、ユーザの認証を行うユーザ認証手段を有するため、下記のような効果を奏する。

【００９２】上記請求項１及び請求項２の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【００９３】請求項４の発明によれば、情報処理装置の前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【００９４】上記請求項１及び請求項２の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【００９５】請求項５の発明によれば、情報処理装置は、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【００９６】上記請求項１乃至請求項４の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構

に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【００９７】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【００９８】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【００９９】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【０１００】請求項６の発明によれば、情報処理装置は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段を有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであるため、下記のような効果を奏する。

【０１０１】リソース識別子としてＵＲＬを利用した場合においても、リソース識別子（ＵＲＬ）の暗号化及び復号を行うことで、上記請求項１乃至請求項５の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【０１０２】請求項７の発明によれば、ネットワークを介してサーバ及びクライアント間で通信可能なネットワークシステムであって、前記クライアント側は、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化手段と、暗号化したリソース識別子を復号鍵に基づき復号する復号手段とを有するため、下記のような効果を奏する。

【０１０３】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【０１０４】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【０１０５】請求項８の発明によれば、ネットワークシステムの前記クライアント側は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ要求手段と、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御手段とを有し、前記サーバ側は、前記ネットワークの上位装置名、アドレス、通信手段を管理するネットワーク管理手段と、該ネットワーク管理手段による通信でデータを配送するデータ配送手段と、サーバ上のデータを管理するデータ管理手段とを有するため、下記のような効果を奏する。

【０１０６】上記請求項７の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【０１０７】請求項９の発明によれば、ネットワークシステムの前記クライアント側は、ユーザの認証を行うユーザ認証手段を有するため、下記のような効果を奏する。

【０１０８】上記請求項７及び請求項８の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【０１０９】請求項１０の発明によれば、ネットワークシステムのクライアント側の前記ユーザ認証手段は、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【０１１０】上記請求項７及び請求項８の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【０１１１】請求項１１の発明によれば、ネットワークシステムの前記クライアント側は、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【０１１２】上記請求項７乃至請求項１０の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【０１１３】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【０１１４】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【０１１５】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【０１１６】請求項１２の発明によれば、ネットワークシステムの前記クライアント側は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理手段を有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであるため、下記のような効果を奏する。

【０１１７】リソース識別子としてＵＲＬを利用した場合においても、リソース識別子（ＵＲＬ）の暗号化及び復号を行うことで、上記請求項７乃至請求項１１の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【０１１８】請求項１３の発明によれば、ネットワークを介してサーバと通信可能な情報処理装置におけるリソース識別子変換方法であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するため、下記のような効果を奏する。

【０１１９】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【０１２０】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【０１２１】請求項１４の発明によれば、リソース識別子変換方法は、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有するため、下記のような効果を奏する。

【０１２２】上記請求項１３の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【０１２３】請求項１５の発明によれば、リソース識別子変換方法は、ユーザの認証を行うユーザ認証ステップを有するため、下記のような効果を奏する。

【０１２４】上記請求項１３及び請求項１４の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【０１２５】請求項１６の発明によれば、リソース識別子変換方法の前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【０１２６】上記請求項１３及び請求項１４の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約でき

る、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【０１２７】請求項１７の発明によれば、リソース識別子変換方法では、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【０１２８】上記請求項１３乃至請求項１６の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【０１２９】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【０１３０】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【０１３１】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【０１３２】請求項１８の発明によれば、リソース識別子変換方法は、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理ステップを有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであるため、下記のような効果を奏する。

【０１３３】リソース識別子としてＵＲＬを利用した場合においても、リソース識別子（ＵＲＬ）の暗号化及び復号を行うことで、上記請求項１３乃至請求項１７の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【０１３４】請求項１９の発明によれば、ネットワークを介してサーバと通信可能な情報処理装置に供給可能な記憶媒体であって、前記ネットワーク上のデータを指定するリソース識別子を暗号化鍵に基づき暗号化する暗号化ステップと、暗号化したリソース識別子を復号鍵に基づき復号する復号ステップとを有するプログラムを記憶しているため、下記のような効果を奏する。

【０１３５】データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できると共に、認証のための公開鍵または秘密鍵を配布する手続きを節約できるという効果がある。

【０１３６】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【０１３７】請求項２０の発明によれば、記憶媒体の前記プログラムは、前記サーバに対しリソース識別子を用いてデータ配送を要求するデータ読出ステップと、前記復号したリソース識別子が正しい場合はリソース識別子を前記サーバに送信し、前記復号したリソース識別子が正しくない場合はリソース識別子の送信を行わない識別子送信制御ステップとを有するため、下記のような効果を奏する。

【０１３８】上記請求項１９の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、ネットワークの通信回数を減らすことにより、ネットワークのトラフィック（通信量）及び通信時間を軽減できるという効果がある。即ち、上述した従来技術と比較すると、本発明では、暗号化されたリソース識別子を使用する場合は、クライアントがリソース識別子を復号し、正しければ復号したリソース識別子をサーバに送信し、正しくなければリソース識別子を送信しないため、通信回数が軽減されるという効果がある。

【０１３９】請求項２１の発明によれば、記憶媒体の前記プログラムは、ユーザの認証を行うユーザ認証ステップを有するため、下記のような効果を奏する。

【０１４０】上記請求項１９及び請求項２０の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【０１４１】請求項２２の発明によれば、記憶媒体の前記ユーザ認証ステップでは、前記暗号化したリソース識別子が正しく復号された場合で且つ前記復号したリソース識別子から前記ネットワークを介してリソースを得られた場合はユーザを認証し、前記暗号化したリソース識別子が得られない場合又は前記暗号化したリソース識別子が正しく復号されない場合又は前記復号したリソース識別子から前記ネットワークを介してリソースを得られない場合はユーザを認証しないため、下記のような効果を奏する。

【０１４２】上記請求項１９及び請求項２０の発明と同様に、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約でき

る、パスワードの盗難といった危険を回避することが可能になる、通信回数が軽減される等の効果がある。

【０１４３】請求項２３の発明によれば、記憶媒体は、パスワードを復号鍵として記憶可能であるため、下記のような効果を奏する。

【０１４４】上記請求項１９乃至請求項２２の発明と同様の効果があるばかりでなく、パスワードを用いた認証機構に対して、パスワードをアクセス毎に入力する手間が軽減されるという効果がある。即ち、上述した従来技術と比較すると、本発明では、クライアントがパスワードを復号鍵として記憶するので、一回だけクライアントにリソース識別子と復号鍵を登録すると、次回からはユーザがパスワードを入力する必要がなくなるという効果がある。

【０１４５】また、パスワードを用いた認証機構に対して、ユーザがパスワードを記憶する必要がなくなるという効果がある。

【０１４６】また、パスワードを用いた認証機構に対して、ユーザがパスワードを誤入力する恐れがなくなるという効果がある。

【０１４７】また、パスワードを用いた認証機構に対して、パスワードをネットワークに流すことがなくなるという効果がある。即ち、上述した従来技術と比較すると、本発明では、パスワードや暗号の暗号化鍵、復号鍵そのものはネットワークに流れないため、従来技術のようなパスワードの盗難といった危険を回避することが可能になるという効果がある。

【０１４８】請求項２４の発明によれば、記憶媒体の前記プログラムは、リソース識別子の入力を促す旨を表示すると共に入力されたリソース識別子を読取り記憶する識別子管理ステップを有し、前記リソース識別子は、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂサーバのアドレスを示すＵＲＬであるため、下記のような効果を奏する。

【０１４９】リソース識別子としてＵＲＬを利用した場合においても、リソース識別子（ＵＲＬ）の暗号化及び復号を行うことで、上記請求項１９乃至請求項２３の発明と同様に、データそのものを暗号化したり復号したりする必要がないため、暗号化及び復号の手続きを節約できる、認証のための公開鍵または秘密鍵を配布する手続きを節約できる、パスワードの盗難といった危険を回避することが可能になる、パスワードを記憶する必要や誤入力する恐れがなくなる、通信回数が軽減される等の効果がある。

【図面の簡単な説明】

【図１】本発明の第１及び第２の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムの要部の構成を示すと共に特許請求の範囲に対応させた機能ブロック図である。

【図２】本発明の第１及び第２の実施の形態に係る情報処理装置の構成を示すブロック図である。

【図３】本発明の第１及び第２の実施の形態に係る情報処理装置（クライアント）及び外部装置（サーバ）からなるネットワークシステムの構成を示すブロック図である。

【図４】本発明の第１の実施の形態に係る情報処理装置における処理を示すフローチャートである。

【図５】本発明の第２の実施の形態に係る情報処理装置における処理を示すフローチャートである。

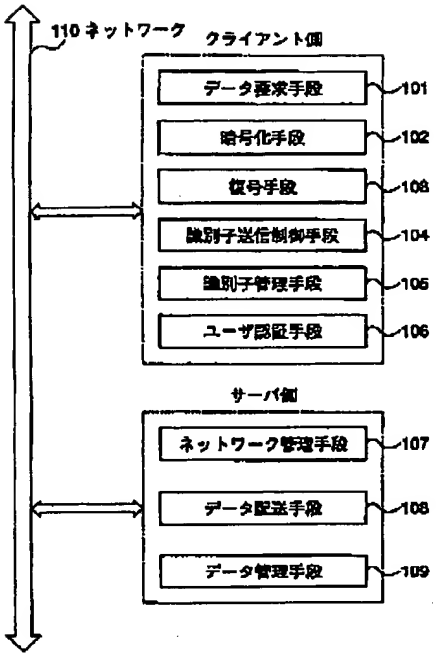
【図６】本発明の第１及び第２の実施の形態に係るプログラム及び関連データを記憶した記憶媒体の記憶内容の構成例を示す説明図である。

【図７】本発明の第１及び第２の実施の形態に係るプログラム及び関連データが記憶媒体から情報処理装置に供給される概念例を示す説明図である。

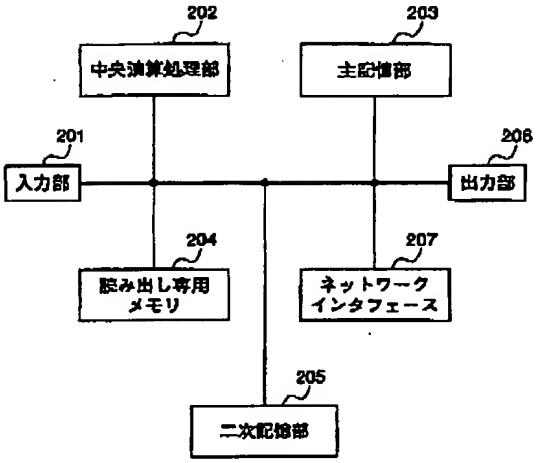
【符号の説明】

１０１　データ要求手段
１０２　暗号化手段
１０３　復号手段
１０４　識別子送信制御手段
１０５　識別子管理手段
１０６　ユーザ認証手段
１０７　ネットワーク管理手段
１０８　データ配送手段
１０９　データ管理手段
１１０、３０７　ネットワーク
２０１　入力部
２０２　中央演算処理部
２０６　出力部
３０１　クライアントプログラム
３０２　暗号化プログラム
３０３　暗号化鍵
３０４　復号プログラム
３０５　復号鍵
３０６、３０８　ネットワークインタフェース
３０９　サーバプログラム
３１０　送信データ

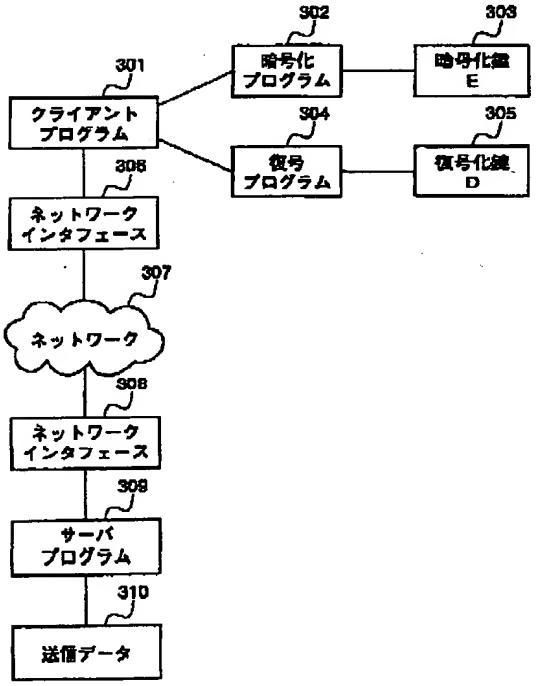
【図１】


110 ネットワーク
クライアント側
データ要求手段
101
暗号化手段
102
復号手段
103
識別子送信制御手段
104
識別子管理手段
105
ユーザ認証手段
106
サーバ側
ネットワーク管理手段
107
データ配送手段
108
データ管理手段
109

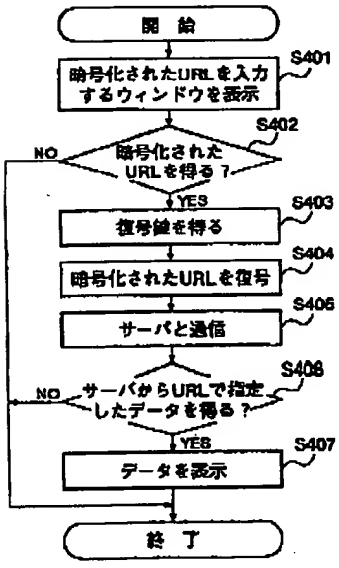
【図２】


202
中央演算処理部
203
主記憶部
201
入力部
206
出力部
204
読み出し専用メモリ
207
ネットワークインタフェース
205
二次記憶部

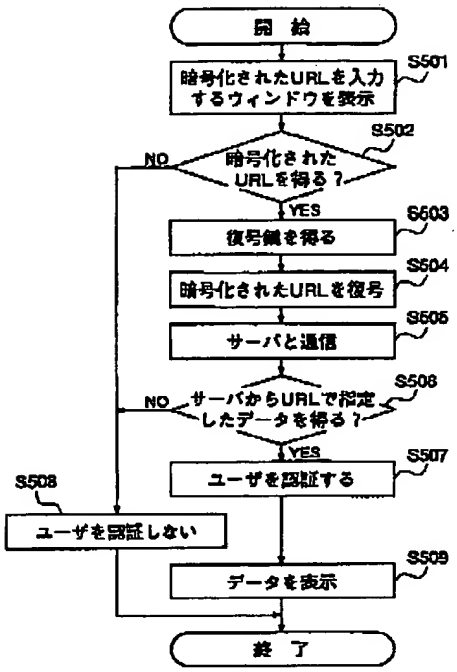
【図３】


302
暗号化プログラム
303
暗号化鍵E
301
クライアントプログラム
304
復号プログラム
305
復号化鍵D
306
ネットワークインタフェース
307
ネットワーク
308
ネットワークインタフェース
309
サーバプログラム
310
送信データ

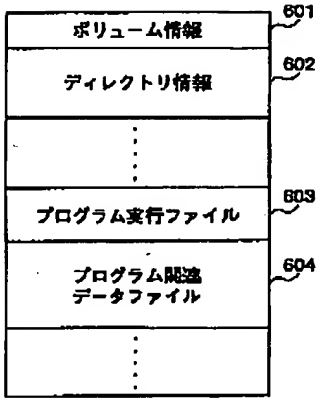
【図４】


開 始
暗号化されたURLを入力するウィンドウを表示
S401
暗号化されたURLを得る？
S402
NO
YES
復号鍵を得る
S403
暗号化されたURLを復号
S404
サーバと通信
S405
サーバからURLで指定したデータを得る？
S406
NO
YES
データを表示
S407
終 了

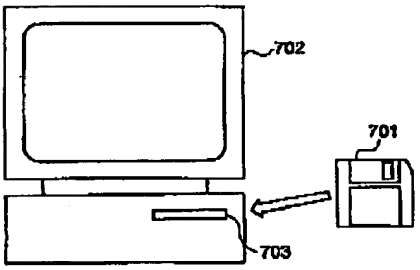
【図５】


開 始
暗号化されたURLを入力するウィンドウを表示
S501
暗号化されたURLを得る？
S502
NO
YES
復号鍵を得る
S503
暗号化されたURLを復号
S504
サーバと通信
S505
サーバからURLで指定したデータを得る？
S506
NO
YES
ユーザを認証する
S507
S508
ユーザを認証しない
データを表示
S509
終 了

【図６】


ボリューム情報
601
ディレクトリ情報
602
プログラム実行ファイル
603
プログラム関連データファイル
604

【図７】


702
701
703